	Application No.	Applicant(s)
Notice of Allowability	10/654,238	WALKER, JESSE R.
	Examiner	Art Unit
	WESLEY L. KIM	2617

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *12/12/07*.

2. ☒ The allowed claim(s) is/are *1,3-5, 7-9, 11-13,15-17, 19-20* .

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) ☐ All.   b) ☐ Some*   c) ☐ None   of the:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
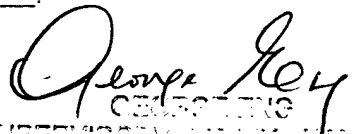
   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application. **THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____ .

   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)

3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date *12/12/07*

4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application

6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .

7. ☐ Examiner's Amendment/Comment

8. ☒ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____ .

DETAILED ACTION

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes

and/or additions be unacceptable to applicant, an amendment may be filed as provided

by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be

submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview

with Rob McDowell on 2/26/08.

The application has been amended as follows:

9. (Currently Amended) An article of manufacture comprising a computer

readable storage medium having stored thereon instructions that, when executed by a

computing computer platform, result in an authenticated key exchange, by:

receiving, by an access point (AP) after distribution of a pairwise master key, a

probe request;

transmitting, by the AP in response to the probe request, a probe response

including an AP nonce generated by the AP; and

receiving, by the AP, a pairwise master key request information element as a

reassociate request from a user station that received the transmitted AP nonce, the

pairwise master key request information element including the AP nonce, a user station

nonce, and a message integrity code, wherein the message integrity code was

computed using a message integrity code algorithm with a key confirmation key, the AP

nonce, and the user station nonce, and wherein the key confirmation key was computed

using a pseudo random function algorithm with the pairwise master key, a media access

control address of the AP, and a media access control address of the user station.

13. (Currently Amended) An article of manufacture comprising a <u>computer</u>

<u>readable</u> storage medium having stored thereon instructions that, when executed by a

~~computing~~ <u>computer</u> platform, result in an authenticated key exchange, by:

transmitting, by an access point (AP) after distribution of a pairwise master key, a

probe request;

receiving, by the user station in response to the probe request, a probe response

including an AP nonce generated by the AP;

transmitting, by the user station, a pairwise master key request information

element as a reassociate request, the pairwise master key request information element

including the AP nonce, a user station nonce, and a message integrity code, wherein

the message integrity code was computed using a message integrity code algorithm

with a key confirmation key, the AP nonce, and the user station nonce, and wherein the

key confirmation key was computed using a pseudo random function algorithm with the

pairwise master key, a media access control address of the AP, and a media access

control address of the user station.

- End of Amendments.

Allowable Subject Matter

1.   Claims 1, 3-5, 7-9, 11-13, 15-17, and 19-20 are allowed.

2.   The following is an examiner's statement of reasons for allowance:

Applicants invention is drawn to utilization of a pairwise master key to generate nonces for authenticated key exchange during a rekeying event in a wireless local area network.

Applicants Claims 1 and 9 each recite, *inter alia*, receiving, by the AP, a pairwise master key request information element as a reassociate request from a user station that received the transmitted AP nonce, the pairwise master key request information element including the AP nonce, a user station nonce, and a message integrity code, wherein the message integrity code was computed using a message integrity code algorithm with a key confirmation key, the AP nonce, and the user station nonce, and wherein the key confirmation key was computed using a pseudo random function algorithm with the pairwise master key, a media access control address of the AP, and a media access control address of the user station. Applicants claims comprise a particular combination of elements, which is neither taught nor suggested by the prior art. Accordingly, applicants claims are allowed for these reasons and for the reasons recited in Amendments filed 12/12/07.

Applicants Claims 5 and 13 each recite, *inter alia*, transmitting, by the user station, a pairwise master key request information element as a reassociate request, the pairwise master key request information element including the AP nonce, a user

station nonce, and a message integrity code, wherein the message integrity code
was computed using a message integrity code algorithm with a key confirmation key,
the AP nonce, and the user station nonce, and wherein the key confirmation key was
computed using a pseudo random function algorithm with the pairwise master key, a
media access control address of the AP, and a media access control address of the
user station. Applicants claims comprise a particular combination of elements, which
is neither taught nor suggested by the prior art. Accordingly, applicants claims are
allowed for these reasons and for the reasons recited in Amendments filed 12/12/07.

Applicants Claim 17 recites, inter alia, a base band processor to; Generate a
probe request to be transmitted to an access point (AP), and to receive a probe
request including an AP nonce generated by the AP; and generate a pairwise
master key request information element including the AP nonce, a user station
nonce, and a message integrity code, the message integrity code being computed
using a message integrity code algorithm with a key confirmation key, the AP
nonce, and the user station nonce, and wherein the key confirmation key is
computed using a pseudo random function algorithm with the pairwise master key, a
media access control address of the AP, and a media access control address of the
user station. Applicants claims comprise a particular combination of elements, which
is neither taught nor suggested by the prior art. Accordingly, applicants claims are
allowed for these reasons and for the reasons recited in Amendments filed 12/12/07.

Dependent Claims 3-4, 7-8, 11-12, 15-16, and 19-20 are allowed as being
dependent on allowed claims 1, 5, 9, 13, and 17.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."
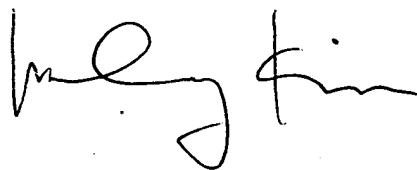
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to WESLEY L. KIM whose telephone number is (571)272-7867. The examiner can normally be reached on Monday-Friday 9:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, George Eng can be reached on 571-272-7495. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

WLK

GEORGE ENG
SUPERVISORY PATENT EXAMINER